**Sfaturi pentru evitarea infectarii PC-ului in timpul Cupei Mondiale**

 [**Sunbelt Software**](http://www.sunbeltsoftware.ro/), important furnizor de solutii de securitate pentru Windows, a publicat o lista de sfaturi pentru managerii companiilor, cat si pentru departamentele de resurse umane, pentru asigurarea conditiilor de siguranta IT la locul de munca a angajatilor in timpul desfasurarii [***Cupei Mondiale***](http://www.fifa.com/worldcup/).

Meciurile de la Cupa Mondiala se vor desfasura in timpul programului companiilor si tot mai multi angajati vor incerca sa urmareasca meciurile, cu sau fara acordul sefilor.

Dorinta tot mai mare de a urmari competitia, chiar si la locul de munca, poate aduce cea mai mare catastrofa de securitate, mai ales ca angajatii ar putea folosi orice mijloace pentru indeplinirea acestei dorinte, iar tot mai multi infractori cibernetici vor profita de aceasta situatie, punand in circulatie malware care va viza „setea” de fotbal.

Astfel, angajatii vor accesa cat mai multe site-uri, in mare parte necunoscute si nesigure, expunand calculatoarele personale la tot mai multe amenintari, sau malware inclus in acele pagini, in banere publicitare sau in codecuri false, virusate, pe care trebuie sa le descarce pentru urmarirea meciurilor.

Astfel, Sunbelt Software apreciaza ca angajatii trebuie sa fie foarte atenti in timpul Cupei Mondiale.

Prima amenintare din lista producatorului de solutii de securitate este aceea a fisierelor infectate raspandite prin mesaje spam care au ca subiect Cupa Mondiala.

Ca la orice eveniment major, fiecare trebuie sa fie foarte atent cand deschide mesaje care au atasamente care sustin ca au ca subiect Cupa Mondiala.

Cel mai probabil, atasamentele vor avea un fisier care ar putea aduce probleme serioase PC-urilor sau retelei. Temele cele mai asteptate sa fie folosite in aceasta campanie vor fi “Free tickets”, “match list”, “watch online” si “tickets refund”, toate proiectate pentru a determina victima sa deschida fisierele respective.

A doua amenintare amintita de Sunbelt Software este motorul de cautare in ale carui rezultate, cel mai probabil, vor fi introduse si link-uri catre site-uri suspecte, care vand cu amanuntul produse de securitate false, cat si produse farmaceutice sau catre pagini care contin fisiere rau intentionate.

Programele antispyware false, care anunta utilizatorii ca au PC-ul infectat si cer pana la 45 de Euro pentru rezolvarea acestei probleme, sunt o mare afacere pentru hackeri, fiind una dintre cele mai folosite metode.

„In cazul in care apare un pop-up care informeaza ca PC-ul este infectat, in timp ce navigati pe internet, si nu provine de la aplicatia de securitate deja instalata, nu va speriati. Pur si simplu deschideti Task Manager (CTRL+ALT+DEL) si inchideti browserul”, spune Sunbelt Software. „Daca o aplicatie suspecta nu a fost instalata si ceea ce vedeti este un simplu pop-up, aceasta procedura va permite sa «scapati» de capcana acelui site”.

O a treia „amenintare” este social networking scams. „Ne asteptam sa fie folosite link-uri suspecte catre Twiter, aplicatii «false» pentru Facebook si altele de acest gen, pe site-urile populare care au la baza web 2.0. Daca vi se cere sa utilizati o aplicatie pe Facebook, nu va temeti ca mai intai sa cautati pe Google, sa va informati daca este o aplicatie legitima sau nu. Sunt multe astfel de aplicatii aparute, care fac parte din arsenalul hackerilor”, spune Sunbelt.

O a patra problema identificata de producatorul de solutii de securitate sunt atacurile care schimba formatul site-urilor. Este trist ca in timpul marilor evenimente, paginile de internet care au legatura cu acesta sunt atacate. In timp ce multe dintre pagini sunt doar schimbate de atacatori, acestia vor, uneori, sa instaleze pe PC-urile vizitatorilor aplicatii rau-voitoare.

„Intotdeauna asigura-te ca aplicatiile de securitate si Windows-ul au update, deoarece exista o multitudine de programe care sunt „sparte” si pe care atacatorii le pot folosi pentru a face rau”, spune Sunbelt.

Deci… atentie maxima!